

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

LISA ADDI, individually and on behalf of all
other persons similarly situated,

Plaintiff,

v.

The International Business Machines, Inc.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Lisa Addi (“Plaintiff”), individually and behalf of all others similarly situated, brings this class action against Defendant The International Business Machines Corporation (“Defendant” or “IBM”). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant for procuring the wiretapping of electronic communications of visitors to Weather.com by third party Oracle America, Inc. (“Oracle”). As alleged below, through its Blue Kai Pixel, Oracle, as procured by IBM, secretly observed, recorded, and otherwise intercepted website visitors’ electronic communications with Defendant and used that data to improve its own marketing and analytical capabilities, as well as those of Defendant. By doing so, Defendant has violated the Maryland Wiretapping and Electronic Surveillance Act, Md. Code Cts. & Jud. Proc. §§ 10-401, *et seq.* (“MWESCA”).

2. During the months of May and June 2023, Plaintiff visited the Website. During these visits, Oracle, as procured by Defendant, recorded and thereby intercepted Plaintiff’s electronic communications in real time with Defendant.

3. Plaintiff brings this action on behalf of herself and a class of all persons whose electronic communications were intercepted by Oracle on the Weather.com website.

PARTIES

4. Plaintiff Lisa Addi is a resident of Maryland and has an intent to remain there and is therefore a citizen of Maryland. On or about May 28, 2023, prior to the filing of this lawsuit, Ms. Addi, who has a Weather.com account, browsed Weather.com on her computer. Ms. Addi was in Maryland when she visited the website. During the visit, Ms. Addi's e-mail address, precise geolocation, and other identifying data were intercepted in real time by Oracle. Ms. Addi was unaware at the time that her e-mail, geolocation, and other identifying data were being intercepted in real-time by Oracle, nor did Ms. Addi meaningfully consent to the same.

5. Defendant IBM is a New York company with its principal place of business at 1 New Orchard Road, Armonk, NY 10504. IBM owns and operates Weather.com. Weather.com was visited over 1.2 billion times in May 2023 alone.¹

6. Defendant procured Oracle Advertising and Customer Experience to manage and collect its website visitors' data.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, and at least one member of the proposed class is citizen of state different from at least one Defendant.

8. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business in New York.

¹ <https://www.similarweb.com/website/weather.com/#overview>

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District.

STATEMENT OF FACTS

I. Oracle Intercepts Communications Between Website Visitors And Websites For Marketing Purposes

10. Oracle is a software-as-a-service company that provides many services and products to businesses and enterprises.

11. One line of products is the “Oracle Advertising and Customer Experience” (“Oracle CX”).

12. Oracle CX is designed to make “every customer interaction matter by connecting all [Oracle CX clients’] business data across advertising, marketing, sales, commerce, and service.”²

13. Oracle CX is used to “[b]uild a complete view of your customer and their every interaction—no matter how, when, where, or with whom they engage.”³

14. Oracle CX offers a marketing tool (“Oracle BlueKai” or “BlueKai”) through which Oracle can collect data on Oracle’s clients’ customers in order to market to and attract new customers.

15. Oracle BlueKai is a data management platform (“DMP”) that “[c]ollects, organizes, and activates audience data from various online, offline, and mobile sources. Using that data, [website owners] can then build detailed customer profiles for targeted advertising and

² <https://www.oracle.com/cx/>

³ *Id.*

personalization initiatives.”⁴

What is a data management platform (DMP) and how does it work?

A DMP collects, organizes, and **activates** audience data from various online, offline, and mobile sources. Using that data, you can then build detailed customer profiles for targeted advertising and personalization initiatives.

Think of a DMP as a large data warehouse where you can store, organize, and analyze all the customer data you’ve collected—including behavioral, geographic, and demographic data. You can gather data directly by adding simple snippets of code called ‘tags’ to your web pages. The DMP will then track the user’s journey.

The insights provided include the URL and keywords and who has visited certain pages. Of course, it can also import data, such as loyalty program profiles, email lists, social media, lead tracking data, and in-person point of sale information—whatever data you have can come together in your DMP.

DMPs then group users with matching or similar attributes into appropriate audience segments. Expand your clearly defined audiences by creating lookalike audiences, which are potential customers with characteristics that match your ideal customer. Then you can use that data to drive personalized and contextual advertising that your customers and prospects are more likely to engage with.

The result? You have a comprehensive snapshot that provides insights on how to best engage with your customers and deliver the level of personalization they demand.

16. Oracle describes Oracle BlueKai DMP “as a large data warehouse where you can store, organize, and analyze all the customer data you’ve collected—including behavioral, geographic, and demographic data. You can gather data directly by adding simple snippets of code called ‘tags’ to your web pages. The DMP will then track the user’s journey.”⁵

17. Oracle BlueKai is designed to “[u]se data to drive personalized and contextual advertising that engages and wins over relevant audiences.”⁶ This is done by “ingest[ing]” website owners’ customer data, “[c]lassify[ing] and organiz[ing] data into targetable user segments,” and serving those customers “third-party datasets” provided by Oracle, who matches those segments with targeted advertising.⁷

⁴ <https://blogs.oracle.com/marketingcloud/post/implement-a-data-management-platform-dmp-to-understand-and-multiply-your-audience>

⁵ *Id.*

⁶ <https://www.oracle.com/cx/marketing/data-management-platform/#documentation>

⁷ *Id.*

18. Oracle BlueKai is also used to “conduct personalized marketing” to prospective customers across their devices on “web and social channels that they spend time on.”⁸

Connect across devices

Create effective cross-device campaigns

Conduct personalized marketing at the individual level with a consistent message across devices.

- Expand your audience by using Oracle ID Graph to bring in third-party data across different marketing channels and devices.
- Use a private ID graph to extend your reach and leverage your ID linkages for cross-device customer targeting.
- Reach your customers/prospects across the open web and social channels that they spend time on by activating the cross-device extension.

19. Oracle BlueKai is also used to import data—which Oracle collects from other Oracle clients’ deployment of BlueKai—to “group users with matching or similar attributes into appropriate audience segments.” Oracle clients can then “use that data to drive personalized and contextual advertising that your customers and prospects are more likely to engage with.”

20. To enable Oracle to track website users, website owners insert a “Core Tag” – “bk-coretag.js” – into their webpages, unbeknownst to the webpage visitor.

21. When a user visits a website that has Core Tag in the code, the user’s browser sends a “GET request” to the website server. The server responds by sending HTML code to the user’s browser. The HTML code includes a JavaScript that contains the Core Tag which instructs the user’s browser to send another GET request to Oracle. Oracle then utilizes the Core Tag to collect data for BlueKai. Through this process, Oracle can extract the website visitor and

⁸ *Id.*


attributes.⁹

22. Oracle intercepts this user data in real-time (*i.e.*, simultaneously with a user's

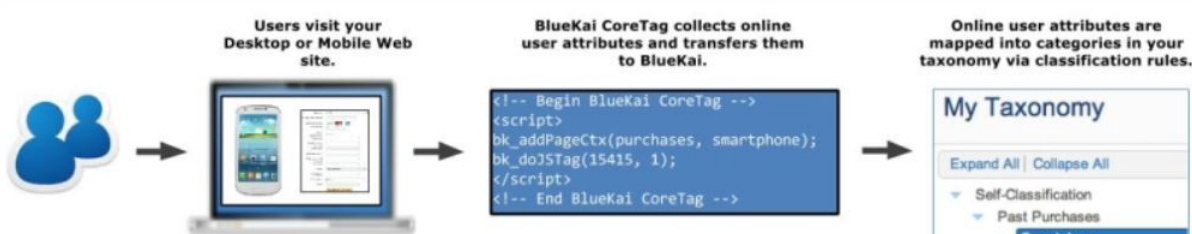
You are here: Integrate > Data Ingest > BlueKai CoreTag

Oracle Data Cloud Core Tag Implementation

You can implement the Oracle Data Cloud CoreTag on your desktop and mobile sites to extract online user attributes and import them into the Oracle Data Cloud platform. The Oracle Data Cloud core tag is an iframe that references the **bk-coretag.js** file, which is a small JavaScript file stored on third-party content delivery networks (CDNs) to facilitate quick access and low latency. The **bk-coretag.js** file includes a library of JavaScript helper functions for setting the source of the iframe and generating the explicit key-value pairs that pass your user attributes to the Oracle Data Cloud platform.

 **Note:** Oracle Data Cloud tags and code include references to BlueKai and bk. These references are the result of legacy naming policies.

When the Oracle Data Cloud core tag is called and the platform receives your online user attributes, classification rules map the collected data into categories (groups of users with the same attribute) in your taxonomy. The following diagram illustrates how the Oracle Data Cloud core tag extracts your online user attributes and imports them into your taxonomy:



```

graph LR
    A[Users visit your Desktop or Mobile Web site.] --> B[BlueKai CoreTag collects online user attributes and transfers them to BlueKai.]
    B --> C[Online user attributes are mapped into categories in your taxonomy via classification rules.]
  
```

The diagram illustrates the process of implementing the Oracle Data Cloud Core Tag. It shows a flow from users visiting a website to the collection of attributes by the BlueKai CoreTag, which then maps these attributes into a taxonomy.

1. **Users visit your Desktop or Mobile Web site.** (Icon: Two people)

2. **BlueKai CoreTag collects online user attributes and transfers them to BlueKai.** (Icon: Laptop showing code)

```

<!-- Begin BlueKai CoreTag -->
<script>
bk_addPageCtx(purchases, smartphone);
bk_do3STag(15415, 1);
</script>
<!-- End BlueKai CoreTag -->
  
```

3. **Online user attributes are mapped into categories in your taxonomy via classification rules.** (Icon: Taxonomy interface)

My Taxonomy

Expand All | Collapse All

- Self-Classification
 - Past Purchases
 - Smartphone

interaction with a website).

23. The data Oracle BlueKai collects that may directly or indirectly identify users

⁹ https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html

includes but is not limited to:

- (a) Geographic location;
- (b) E-mail address;
- (c) Demographic information such as gender, age, and income range;
- (d) IP address;
- (e) HTML page properties;
- (f) Pages viewed;
- (g) Purchase intent¹⁰;
- (h) Add-to-cart actions;
- (i) Keystrokes;
- (j) Search terms entered; and
- (k) “Mouse click events”¹¹

24. After extracting user data from a website, Oracle’s Core Tag creates and sends a “unique user ID” to Oracle’s “Data Cloud” platform “so [the ID] can be synchronized to the network of user profiles that are linked together in the Oracle ID Graph.”

//

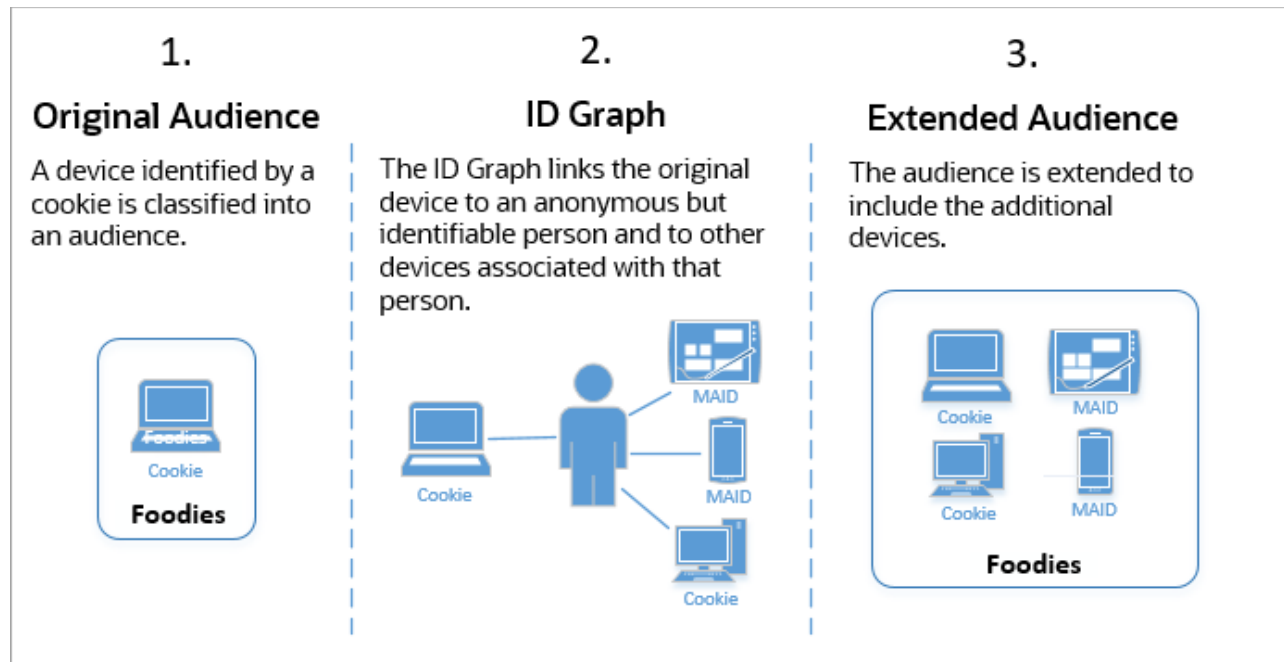
//

//

//

¹⁰ “Purchase behavior insights enables [website owners] to understand your audience’s buying habits, based on actual purchase data sourced from Oracle Data Cloud partners.” *See* https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/AudienceInsights/insights_data.html?Highlight=purchase%20intent.

¹¹ https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/ManagingTags/CreatingContainers/capture_mouse_clicks.html



25. Oracle's ID Graph is used to identify users who utilize different devices. "The Oracle ID Graph helps marketers connect identities across disparate marketing channels and devices to one customer."¹²

//

//

//

//

//

//

//

//

//

¹² https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/id_management.html#oidg

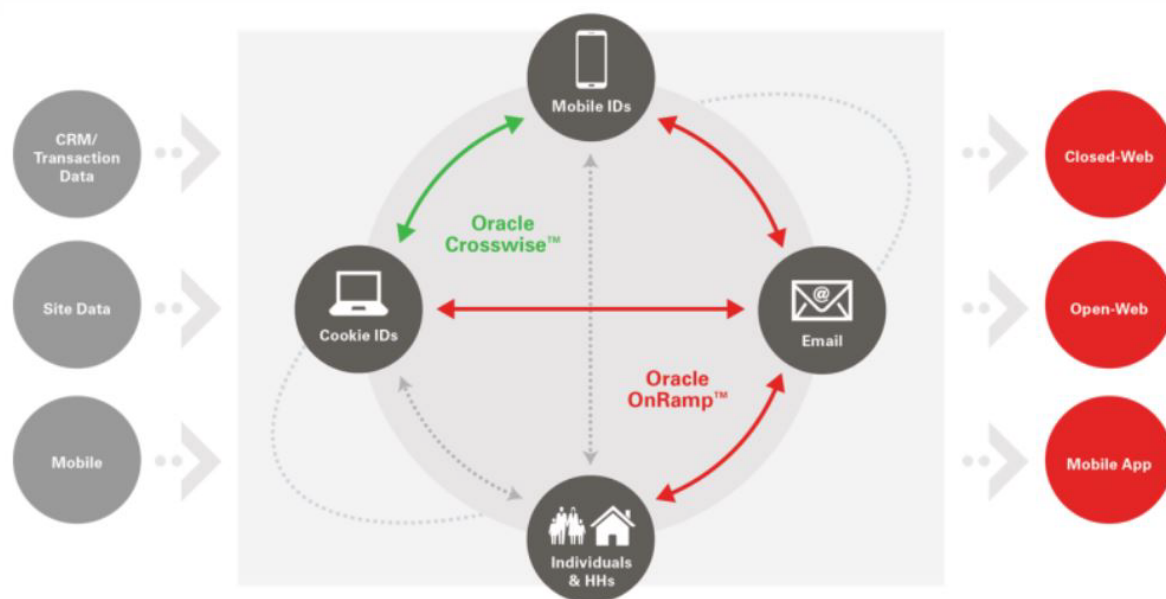
Oracle ID Graph accurately links these ID sources and validates them against high-quality data known to be true because it is made up of verified transaction and subscription data.

Using the Oracle ID Graph

The Oracle ID Graph helps marketers connect identities across disparate marketing channels and devices to one customer. Powered by the Oracle Marketing Cloud and Oracle Data Cloud, the Oracle ID Graph seamlessly pulls together the many IDs across marketing channels and devices that comprise a given person, enabling marketers to tie their interactions to an actionable customer profile. This ID enables the marketer to orchestrate a relevant, personalized experience for each individual across marketing channels and device types.

Optimize cross-channel orchestration

Oracle ID Graph powers linkages to enable identity solutions for cross-channel targeting.



Improve cross-channel targeting

Many customers research on one device but use another to purchase. With the Oracle ID Graph, customers are more likely to receive a relevant experience as they move between devices. For example, if a customer uses a desktop browser to search for flights, an airline marketer can ensure a relevant ad appears for a flight promotion when that same customer switches to their mobile device. This results in a higher conversion rate and more optimized budgets.

26. Oracle correlates visitors' web activity with the ID and creates a "segment" profile of the visitor. Oracle then feeds the visitor advertisements that match the visitor's purported segment profile. Oracle offers "more than 30,000 data attributes" to Oracle clients so to "power" their "direct marketing initiatives and let [them] connect with [their] target audience anywhere on the internet."¹³

27. Oracle boasts providing "actionable audience data on more than 300 million users", which is "80% of the entire US internet population at [Oracle subscribers'] fingertips."¹⁴

28. This data includes in part "age, gender, employment, language, family composition, household income and net worth" and is "self-declared" – not just inferred.¹⁵

29. Oracle maintains a symbiotic relationship with their clients. Oracle does not simply manage their clients' data; Oracle also retains and uses the same data to assist other clients. With each piece of data Oracle collects, the BlueKai profiling software becomes even more useful. Because BlueKai's success depends on their data accumulation, Oracle does not merely profit monetarily from each client, but also builds BlueKai's profiling apparatus.

30. To summarize, website owners add a Core Tag onto their websites, which enables Oracle BlueKai to collect significant identifying information. Oracle then associates that data to a specific user, compiles that data with other data about the user Oracle has in its possession, and provides that data to website owners to enable website owners to hyper target users in marketing campaigns. Oracle then retains that data and uses it to assist other website owners.

II. Oracle, As Procured By Defendant, Intercept Communications On Weather.com Between Visitors And Defendant, Including Plaintiff

¹³ <https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html>

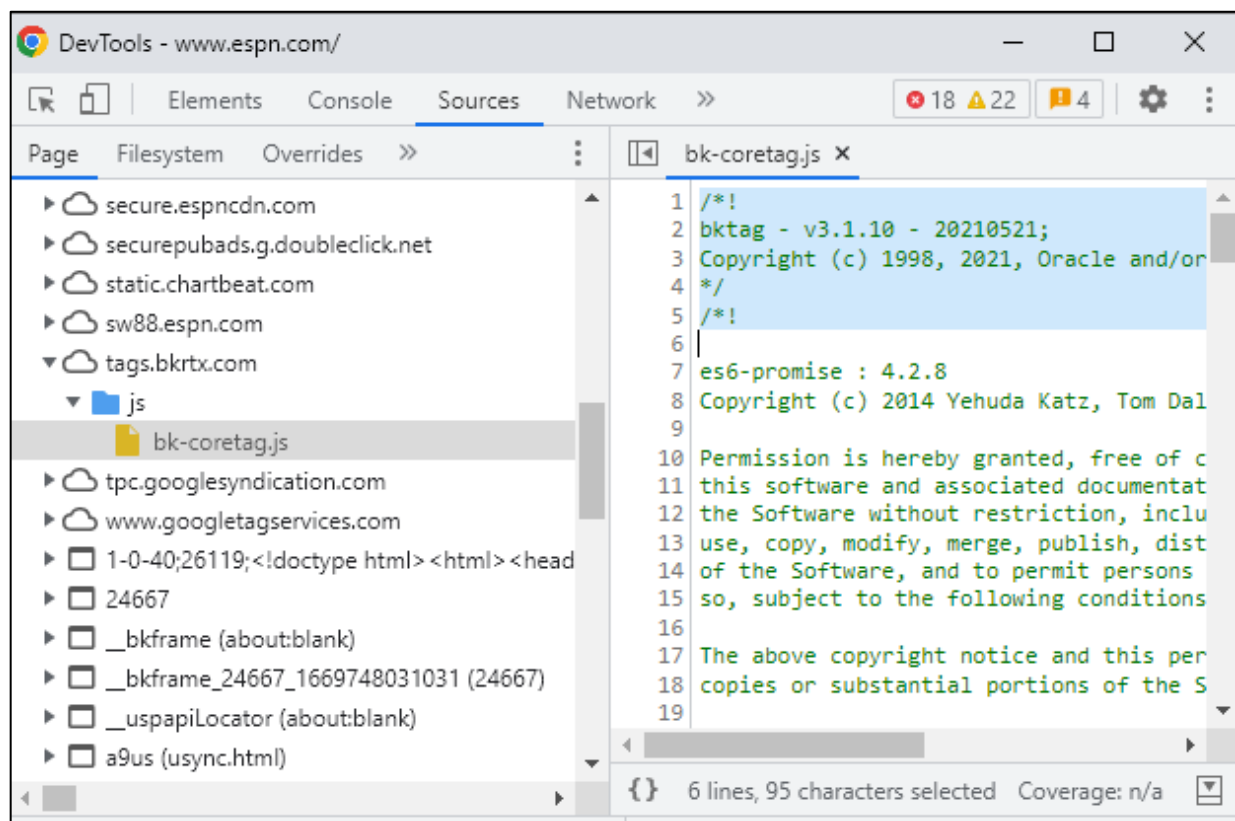
¹⁴ *Id.*

¹⁵ *Id.*

31. Defendant owns and operates the Weather.com website.

32. Defendant willfully enabled, allowed, or otherwise procured Oracle to intercept communications between Defendant and visitors to the Weather.com website through a contractual arrangement.

33. Defendant procured Oracle to embed the bk-coretag.js CoreTag JavaScript on the Weather.com website.



34. BlueKai operates on Weather.com in the same manner as alleged above.

35. Through the BlueKai Core Tag, Oracle collected at least the following information from all Weather.com website visitors:

- (a) Precise geolocation data;
- (b) IP Address;
- (c) Website document location;

- (d) Website referrer;
- (e) Website title;
- (f) HTML page properties;
- (g) Add-cart actions;
- (h) Keystrokes;
- (i) Search terms; and
- (j) Mouse click events.

36. In addition to items (a) – (j) above, through the BlueKai Core Tag, Oracle collected the e-mail address and first name from Weather.com website visitors who created an account.

37. Plaintiff and other Class Members accessed Weather.com in Maryland. Upon accessing the website in Maryland, the browser sent a GET request from Maryland to the Weather.com website's servers. The Weather.com website then sent a signal to web browser instructing the browser in Maryland to send another GET request to Oracle. The web browser then sent another GET request from Maryland to Oracle, which then began tracking Plaintiff's and Class Members' communications on Weather.com.

38. When Plaintiff and other Class Members visited Weather.com, the contents of their website communications – namely, the identifying information alleged above – were intercepted in real-time by Oracle as procured by Defendant. Oracle then used that data to create IDs for each website visitor, including Plaintiff, and to target advertisements to Plaintiff and other website visitors. Upon information and belief, Oracle also retained this information and subsequently provided it to other website owners to assist these other website owners in their marketing efforts.

39. The precise geolocation and e-mail addresses intercepted by Oracle here are

sufficient to identify Plaintiff and other Class Members.

40. Precise geolocation can be used by anyone to uniquely identify a person. A study in 2013, for example, analyzed mobility data for 1.5 million people, finding that researchers needed only four randomly chosen spatio-temporal points (points that represent the time and location of a specific event, such as watching a video) to uniquely identify 95% of the people (approximately 1.425 million out of 1.5 million) in the dataset.¹⁶

41. This data may also be used to track consumers to sensitive locations, including places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, and welfare and homeless shelters.

42. By plotting the latitude and longitude coordinates including geolocation data using publicly available map programs, it is possible to identify which consumers' mobile devices visited reproductive health clinics. Similar methods may be used to trace consumers' visits to other sensitive locations.

43. As Paul Ohm, a law professor and privacy researcher at Georgetown University Law Center, explains it: “[r]eally precise, longitudinal geolocation information is absolutely impossible to anonymize.”¹⁷ In fact, out of all identifiers, “D.N.A. is probably the only thing that’s harder to anonymize than precise geolocation information.”¹⁸

44. Defendant procures Oracle to collect this geolocation data to enhance Defendant’s and Oracle’s marketing efforts, its advertising profits, and its app analytics.

¹⁶ Yves-Alexandre de Montjaye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, SCIENTIFIC REPORTS 2 (Feb. 4, 2013), <https://www.nature.com/articles/srep01376>.

¹⁷ Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy* N.Y. TIMES (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.

¹⁸ *Id.*

45. Companies collect and disclose geolocation so they can maximize their advertising revenue. As a *New York Times* article explained: “For brands, following someone’s precise movement is key to understanding the ‘customer’s journey’—every step of the process from seeing an ad to buying a product.”

46. Marketers consider geolocation “the Holy Grail of advertising” because it creates “the complete picture that connects all of our interests and online activity with our real-world actions.”¹⁹

47. Thus, by intercepting precise geolocation data, Oracle, as procured by Defendant, intercepts information concerning the identity of the parties to a communication, as such data can be used to identify individual users.

48. Similarly, as industry leaders,²⁰ trade groups,²¹ and courts²² agree, an e-mail address constitutes information sufficient to identify individual persons. Indeed, multiple services exist for pairing an email address to an identity that are accessible to ordinary people.²³

49. Thus, by intercepting e-mail addresses, Oracle, as procured by Defendant, intercepts information concerning the identity of the parties to a communication, as such data can be used to identify individual users.

¹⁹ *Id.*

²⁰ Allison Schiff, *Can Email Be The Next Big Online Identifier?*, AD EXCHANGER (Aug. 25, 2020), <https://www.adexchanger.com/data-exchanges/can-email-be-the-next-big-online-identifier/> (quoting Tom Kershaw, CTO of Magnite, who said “[a]n email address is universally considered to be PII, so as such it can never be a valid identifier for online advertising”);

²¹ NETWORK ADVERTISING INITIATIVE, NAI CODE OF CONDUCT 19 (2019), https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf (identifying email as PII).

²² *See, e.g., United States v. Hastie*, 854 F.3d 1298, 1303 (11th Cir. 2017) (“Email addresses fall within the ordinary meaning of information that identifies an individual. They can prove or establish the identity of an individual.”)

²³ *See, e.g., BEENVERIFIED*, <https://www.beenverified.com/>.

CLASS ALLEGATIONS

50. Pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3), Plaintiff seeks to represent a class of all Maryland residents who visited Weather.com in Maryland during the statute of limitations period and whose electronic communications were intercepted or recorded by Oracle (the “Class”).

51. Plaintiff reserves the right to modify the class definition as appropriate based on further investigation and discovery obtained in the case.

52. Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class Members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

53. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendants have violated the MWESCA, and whether class members are entitled to actual and/or statutory damages for the aforementioned violations.

54. The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, visited the Weather.com in Maryland and had their electronic communications intercepted and disclosed to Oracle in Maryland through the use of Oracle’s wiretaps.

55. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class Members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this

action vigorously. The interests of Class Members will be fairly and adequately protected by Plaintiff and her counsel.

56. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class Members. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

57. Plaintiff brings all claims in this action individually and on behalf of members of the Class against Defendant.

CAUSES OF ACTION
COUNT I

**Violation of The Maryland Wiretapping and Electronic Surveillance Act,
Md. Code Cts. & Jud. Proc. §§ 10-401, *et seq.***

58. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

59. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

60. The MWESCA makes it unlawful for any person to "[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire,

oral, or electronic communication.” Md. Code Cts. & Jud. Proc. § 10-402(a)(1).

61. In the context of the MWESCA, “willfully” is defined as “an intentional violation or a reckless disregard of a known legal duty.” *Benford v. Am. Broadcasting Co.*, 649 F. Supp. 9, 10 (D. Md. 1986).

62. “Electronic communication” is defined as “[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.” Md. Code Cts. & Jud. Proc. § 10-401(5)(i).

63. “Intercept” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Md. Code Cts. & Jud. Proc. § 10-401(4).

64. “Contents” is defined as “any information concerning *the identity of the parties to the communication* or the existence, substance, purport, or meaning of that communication.” Md. Code Cts. & Jud. Proc. § 10-401(7) (emphasis added).

65. As alleged above, Oracle intercepted Plaintiff’s and Class Members’ electronic communications because Oracle BlueKai “reroute[d] communications to an interceptor,” Oracle. *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 130 (3d Cir. 2022); *see also Katz-Lacabe v. Oracle America, Inc.*, --- F. Supp. 3d ---, 2023 WL 2838118, at *9 (N.D. Cal. Apr. 6, 2023) (finding plaintiffs sufficiently alleged Oracle was a third-party wiretapper under California law).

66. Further, as alleged above, Oracle intercepted the “contents” of Plaintiff’s and the Class’s electronic communications with Defendant because Oracle intercepted information concerning “the identity of the parties to the communication” (*i.e.*, the geolocation and e-mails of Plaintiff and other Class Members, which is sufficient to identify them).

67. Plaintiff's and Class Members' electronic communications were intercepted in Maryland, which is "the point at which the signals [*i.e.*, Plaintiff's and the Class's electronic communications] were routed to [Oracle's] servers." *Popa*, 52 F.4th at 132.

68. At all relevant times, Defendant procured Oracle to intercept Plaintiff's and Class Members' electronic communications with Weather.com.

69. Defendant sought to profit and in fact did profit off procuring the interception of Plaintiff's and the Class's electronic communications while intentionally or recklessly disregarding its known legal duty.

70. Specifically, Defendant was enriched when it utilized Plaintiff's and Class members' personal information for its own financial advantage to optimize its own platform, including by allowing its partners to target Plaintiff and Class members for lucrative advertisements. Defendant also profited when it utilized Plaintiff's and Class members' personal information stored without meaningful consent for its own financial advantage to build better services, to maintain and improve its services, to develop new services, and to measure performance, all of which enable Defendant to create operational efficiencies and be competitive in a wide array of industries.

71. In exchange for Plaintiff's and Class members' loss of privacy and the financial benefits Defendant enjoyed as a result thereof, including, but not limited to, advertising profits, while Plaintiff and Class members received nothing.

72. Plaintiff and Class Members did not meaningfully consent to Defendant's actions in procuring Oracle to wiretap visitors to Weather.com. Nor did Plaintiff or Class Members meaningfully consent to Oracle's intentional access, interception, reading, learning, recording, and collecting of Plaintiff's and Class Members' electronic communications.

73. The violation of MWESCA constitutes an invasion of privacy sufficient to confer Article III standing. *See, e.g., In re Facebook Internet Tracking Litigation*, 956 F.3d 589, 598-99 (9th Cir. 2020).

74. Plaintiff and Class Members seek all relief available under Md. Code Cts. & Jud. Proc. §§ 10-410(a)(1)-(3), including statutory damages of \$100 dollars per day for each day of violation or \$1,000, whichever is higher, punitive damages, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

- (a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;
- (b) For an order declaring the Defendant's conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;
- (e) For prejudgment interest in all amounts awarded;
- (f) For an order of restitution and all other forms of equitable monetary relief;
- (g) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and cost of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: June 20, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ Julian C. Diamond

Julian C. Diamond

Joseph I. Marchese

Max S. Roberts

Julian C. Diamond

1330 Avenue of the Americas, 32nd Floor

New York, NY 10019

Telephone: (646) 837-7150

Facsimile: (212) 989-9163

E-Mail: jmarchese@bursor.com

mroberts@bursor.com

jdiamond@bursor.com

BURSOR & FISHER, P.A.

Christopher R. Reilly (*Pro Hac Vice forthcoming*)

701 Brickell Ave., Suite 1420

Miami, FL 33131

Telephone: (305) 330-5512

Facsimile: (305) 676-9006

E-Mail: creilly@bursor.com

Attorneys for Plaintiff